
United States District Court

DISTRICT OF COLORADO

UNITED STATES OF AMERICA

CRIMINAL COMPLAINT

v.

CASE NUMBER:

DAVID PAUL MOE

12-mj-01100-KMT

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

COUNT ONE

On or about May 4, 2012, in the State and District of Colorado, DAVID PAUL MOE, defendant herein, knowingly distributed and attempted to distribute child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), that has been mailed, and, using any means and facility of interstate and foreign commerce, shipped and transported in and affecting interstate and foreign commerce by any means, including by computer.

All in violation of Title 18, United States Code, Section 2252A(a)(2) and (b)(1).

COUNT TWO

On or about July 24, 2012, in the State and District of Colorado, DAVID PAUL MOE, defendant herein, did knowingly possess any computer disk and other material that contained an image of child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), that has been mailed, and shipped and transported in interstate and foreign commerce by any means, including by computer, and that was produced using materials that have been mailed, and shipped and transported in interstate and foreign commerce by any means, including by computer.

All in violation of Title 18, United States Code, Section 2252A(a)(5)(B) and (b)(2).

//

//

//

//

//

I further state that I am a Special Agent with Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and that this complaint is based on the following facts: see Affidavit attached hereto and herein incorporated by reference.

Continued on the attached sheet and made a part hereof: X Yes No

 s/Melissa Coffey

Signature of Complainant

Sworn to before me

Jul 24, 2012 6:33 pm

Date

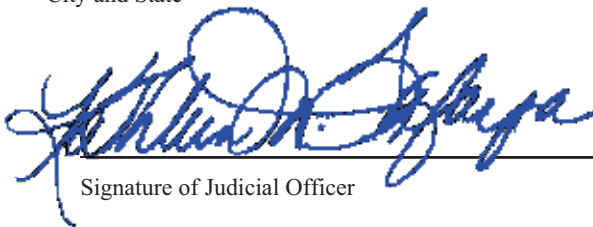
at Denver, Colorado

City and State

Kathleen M. Tafoya
United States Magistrate Judge

UNITED STATES MAGISTRATE JUDGE

Name and Title of Judicial Officer



Signature of Judicial Officer

AFFIDAVIT

I, Special Agent Melissa Coffey of United States Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am assigned to the Special Agent in Charge (SAC), Denver, Colorado. I have been so employed since July, 2006. I have successfully completed the Criminal Investigator Training Program and Special Agent Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. Prior to July, 2006, I was employed by U.S. Customs and Border Protection (and a predecessor agency, the Immigration and Naturalization Service (INS)) for over three (3) years. I have a Bachelor of Arts degree in Criminal Justice. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have received training and instruction in the field of investigation of child pornography and have had the opportunity to participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as storage devices, the Internet, and printed images).
2. This affidavit is submitted in support of an application of a complaint for the arrest of David Paul Moe, for violations of Title 18, United States Code, Sections 2252A(a)(2), distribution of child pornography, and 2252A(a)(5)(b), possession of child pornography.
3. Because this affidavit is being submitted for the limited purpose of securing a complaint, I have not included each and every fact known to me concerning this investigation.
4. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

RELEVANT STATUTES

5. This investigation concerns alleged violations of 18 U.S.C. Sections 2252A(a)(2) and (a)(5)(b), relating to distribution, attempted distribution, and possession of child pornography.

DEFINITIONS

6. The following definitions apply to this Affidavit.
7. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

8. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image See 18 U.S.C. § 2256(5).
9. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

INVESTIGATION

10. On or about January 13, 2011, in an undercover capacity, ICE SA Eric Sajo of the SAC San Diego Cyber Crimes Unit identified a website link posted on "Website A." Names of websites have been changed in this affidavit to protect an ongoing investigation. SA Sajo clicked on the link and identified an image board. The user can choose to enter a name, subject and text but the website does not require the user to do so prior to posting an image. Below are three examples of images posted on "Website B:"
 - A. Posted 2011-01-13 11:10:57: This image depicts a minor female child approximately eight (8) years old. The female child is nude from the waist down wearing a pink and white shirt. The female child is lying on a bed with both legs spread towards the camera. The female child's legs are raised as she spreads her vaginal area with both of her hands. The female child's vaginal area is completely exposed.
 - B. Posted 2011-01-13 11:14:21: This image depicts two minor female children approximately six (6) to eight (8) years old lying on a bed. One female child is lying on her back wearing a pink dress and thigh high white stockings. The pink dress is pulled up to her waist exposing her vaginal area. The second child in the picture is lying on top with her head towards and facing the other female child's vaginal area. The second female child is wearing a red top with a white headband. The second child appears to be performing oral copulation on the other female child with her tongue on or near the other female child's vagina.
 - C. Posted by "Anonymous" 2011-01-13 11:26:03: This image depicts a minor female child approximately eight (8) to ten (10) years old. The female child is naked from her midsection up and is lying on a bed. The female child's left hand is covering her left breast and her right breast is exposed. The female child has what appears to be male ejaculate on her face, nose and mouth.
11. Further investigation caused SA Sajo to apply for a federal search warrant in the Southern District of California on February 8, 2011, for website content located in the Southern District of Texas for violations of 18 United States Code 2252, et. seq – Possession of Child Pornography. The search warrant return of evidence consisted of approximately 861 suspect child pornography files located in image Directory 55 of "Website B" and web access log information for images posted to the website.
12. On April 6, 2011, SA Sajo was supplied with a matched entry text document which separated IP logs with "GET" requests. "GET" requests are generated when a user's web browser requests/accesses a file from the website to specified images of Directory 55. The evidence obtained from "Website B" was only from January 16, 2011, due to web server configuration. The IP log information for January 16, 2011, identified that the user successfully viewed suspect child pornography images contained in Directory 55. The log files also identify the frequency of successful (GET) requests for the suspect images, which provide evidence that the user intended to view the content. The viewable thumbnail(s) as displayed on the message board webpage are large enough to identify the image content without clicking on the image to enlarge. The web

access logs from this website indicate when a user accessed the website and the specific files the user accessed and received, or attempted to receive. Each web page captured displayed approximately thirty (30) or fewer images.

13. A review of the web access logs received from “Website B” identified a user assigned IP address 174.51.44.108 who accessed “Website B” and viewed numerous visual depictions of minors engaged in sexually explicit conduct. Although there is no record that the user accessed an enlarged (full size) image, the logs show approximately 502 incidents of access of thumbnail images by the user. The thumbnail images, as displayed, were of sufficient size for a user to identify the nature and content of the images. Below are three examples of images accessed by the user assigned IP address 174.51.44.108 at the specified date and time:
 - A. 174.51.44.108 - - [16/Jan/2011:21:26:05 -0600] APeVArO8I7Ep.jpg: This image depicts a pre-pubescent female minor lying naked on her back. Her legs are spread open and an adult penis is penetrating her vagina. The marking “Maxxx.”, followed by non-English characters are written on her stomach. The image has a date stamp in the lower right corner of “18/05/2008.”
 - B. 174.51.44.108 - - [16/Jan/2011:21:27:13 -0600] aQOrAYO9etef.jpg: This image depicts a pre-pubescent female minor lying naked on her back. Her legs are spread open and what appears to be a red object is penetrating her vagina and a red ball gag has been inserted in her mouth and tied around her head.
 - C. 174.51.44.108 - - [16/Jan/2011:21:27:07 -0600] ike4EhEGANe3.jpg: This image depicts a pre-pubescent female minor lying naked on her back. An adult penis is anally penetrating the minor.
14. SA Sajo queried IP address 174.51.44.108 in a law enforcement database which identified at least thirteen (13) dates between December 17, 2010 and March 28, 2011 that the IP address was active on the eDonkey P2P file sharing network. During this time period, a user assigned IP address 174.51.44.108 had available for download several files with names indicative of child pornography such as: “[PTHC] 7yo Strip Show at the Piano.avi”, “Tara 8yo_ Sucking Daddy\s.mpg” and “Kinderkutje Valya-44 Fucking A 8-10Yo Hot!!!.avi.” On March 28, 2011, at approximately 05:32 GMT, a computer assigned IP address 174.51.44.108 and operating on the eDonkey network was identified as having available a file entitled “Mes4 - 9y girl fingered 17y boy & man (DX5) (16m 36s).avi” with a digital signature, also known as MD4 hash value of ‘AD70AB410FD2918B98A67731EBAB5283’. Your Affiant viewed a copy of the file, with a digital signature translated to a SHA1, which was obtained by law enforcement during previous investigations. The file is a video, approximately sixteen (16) minutes and thirty-six (36) seconds in length. The video begins with a pre-pubescent female minor lying naked on what appears to be a bed. Hands are seen touching the female’s body and vagina. At approximately one minute and twenty-two (22) seconds the video goes blank and restarts at approximately two (2) minutes and forty-five (45) seconds. The video continues with the same female minor and a naked male minor engaged in oral-genital sexual intercourse under 18 U.S.C. § 2256(2)(A)(i) (the female minor performs oral sex on the male and the male minor performs oral sex on the female).
15. On July 8, 2011, 2012, HSI SAC San Diego SA Eric Sajo sent a DHS Summons to Comcast Cable Communications for subscriber records pertaining information for IP address 174.51.44.108 on 01/16/2011 at 17:01:52-0600 CST. On August 1, 2011, HSI SAC San Diego SA Eric Sajo sent a DHS Summons to Comcast Cable Communications for subscriber information for IP address 174.51.44.108 from 03/28/2011 to 03/30/2011. Comcast records identified customer David Moe was assigned the IP address 174.51.44.108

from 01/01/2011 at 06:18:37 GMT to 03/31/2011 at 07:00:02 GMT. For both dates, Comcast confirmed David Moe, 8034 East Fairmount Drive, Denver, CO, 80230, as the subscriber for the Internet service.

16. An investigative lead from SAC San Diego was received by HSI SAC Denver identifying David Moe as a suspected subscriber to "Website B" and to a P2P file sharing network.
17. Based upon my knowledge, training and experience and the experience of other law enforcement personnel, I have learned that computers on peer to peer file sharing networks have software installed on them that facilitate the trading of electronic files. Peer to Peer (hereinafter referred to as "P2P") file sharing is a method of communication available to Internet users through the use of specialized software. Computers with P2P software installed use the Internet as a conduit for communicating with each other. This communication is frequently in the form of file sharing. Several different P2P software packages are available for download over the Internet. Some P2P software packages are compatible with others, but not all are compatible. Compatible P2P software packages effectively create a P2P "network." In general, P2P software allows the user to specify a folder on the computer in which to place files to be shared with other users on a P2P network. A user can obtain files by opening the P2P software on their computer and conducting a search of the files currently being shared by other users on the network. P2P software usually allows the user to search these files for keywords. The results of the keyword search are then displayed to the user and the user can select the file(s) to download from the list. The download of a file is achieved through direct connections with at least one of the computers offering to share the file selected for download by the user.
18. Based on information provided by Detective Brian Koopman of the Loveland Police Department, who is an active participant in the Internet Crimes Against Children (ICAC) Task Force, I have learned information specifically related to computers on the eDonkey2000 (hereinafter referred to as "eD2k"), and Kademia (hereinafter referred to as "Kad") peer to peer file sharing networks.
 - A. A commonly used P2P client software program is eMule. eMule is a free Microsoft Windows P2P client software program for the eD2k and Kad file sharing networks. Typically, when a user launches the eMule client program, the client program will likely connect to an eD2k network server. Once connected to an eD2k server, information about the files the user is sharing is provided to that server. Such information may include the file's eD2k hash value, the file's size, and parsed keyword terms from the file name. The eD2k network uses the MD4 hash algorithm to uniquely identify files on the network.
 - B. Files on the eDonkey network are uniquely identified using Message-Digest Algorithm (MD4) root hash of a MD4 hash list of the file. Files with identical content but different names are treated as the same file, and files with different contents but the same name are treated as different. Your Affiant knows through the computer forensic community that there has never been a documented occurrence of two different files being found on the Internet having different contents to share the same hash value.
 - C. A investigative method allows investigators the ability, while adhering to the eD2k network protocols, to search for files they believe to be child pornography, if they know the files eD2k MD4 hash value and file size. During this type of search, the investigator can query eD2k network servers for client users who have recently reported to eD2k network servers that they have a file, in whole or in part, that matches a known eD2k MD4 hash value of a file an investigator believes to be child pornography. The eD2k network servers will respond with matching results, which include the

client or clients' IP address (es). This is based on the eD2k MD4 hash value, as recently reported by the client to the eD2k network servers, regardless of the file name associated with that file.

- D. Although transparent to the typical user, when searches are conducted, additional results are received from the eD2k servers or other clients, which may include the eD2k MD4 hash value of the file, the file size, and the IP addresses of clients who recently reported to the network as having that file in whole or in part. This information can be documented by investigators and compared to those eD2k MD4 hash values the investigator has obtained in the past and believes to be child pornography. This allows for the detection and investigation of computers involved in possessing, receiving, and/or distributing files of previously identified child pornography. Therefore, without even downloading the file, the investigator can compare the eD2k MD4 hash value to the hash value of an image or video depicting child pornography previously identified by law enforcement and determine with mathematical certainty that a file seen on the network is an identical copy of a child pornography file law enforcement has seen before.

19. On June 14, 2012, your Affiant contacted the Colorado Division of Labor and Employment and requested a wage report from December 2010 to the present for the Social Security Number (SSN) associated with Moe. Wages for the SSN were reported at Paddington Station, 1301 Quebec Street, Denver, Colorado 80220.
20. On June 14, 2012, your Affiant conducted a search on Google.com and identified Paddington Station Preschool located at 1301 Quebec Street, Denver, Colorado 80220. Your Affiant reviewed the preschool's website, www.paddingtonstation.org, and located a photograph of David Moe. According to the preschool's website on that date, David Moe teaches Cultural Rhythms/Enrichments (3-5 year olds) and has been the Director of Enrichments and Before and After-School Care programs since 2005. It additionally states that Mr. Moe participated in the Stanley British Primary Teacher Preparation Program.
21. On June 14, 2012, your Affiant conducted record checks of the Colorado Division of Motor Vehicle (DMV) records and located a current valid Colorado driver's license issued in November 2011 to David Moe at 8034 East Fairmount Drive, Denver, Colorado 80230.
22. On June 19, 2012, your Affiant requested and received a copy of Moe's driver's license. The driver's license photograph appears to be the same person identified as David Moe on the Paddington Station Preschool's website.
23. On June 28, 2012, your Affiant sent a DHS Summons to Comcast Cable Communications for subscriber records pertaining to 8034 East Fairmount Drive, Denver, Colorado 80230. Comcast Cable Communications return identified David Moe as the subscriber for the Internet service. Comcast records identified customer David Moe was assigned the IP address 174.51.59.13 from April 22, 2012 – June 27, 2012 and the IP address 174.51.72.232 from December 28, 2011 – April 24, 2012.
24. On July 13, 2012, your Affiant spoke to Detective Brian Koopman with the Loveland Police Department and member of the Internet Crimes Against Children (ICAC) Task Force and learned the following:
 - A. On May 4, 2012, at approximately 10:06:13 hours (UTC), working in an official undercover capacity, Detective Koopman connected to the eD2k and Kad networks through the Internet using an eD2k/Kad P2P client program. At approximately 10:06:13 hours (UTC), Detective Koopman observed a computer that was recently reporting that it was sharing at least one image file believed

to contain child pornography. Detective Koopman observed this host computer to have an IP address of 174.51.59.13.

- B. On May 4, 2012, at approximately 21:37:00 hours (UTC), Detective Koopman attempted to download a digital .avi file believed to contain child pornography from the remote host computer located at IP Address 174.51.59.13. Detective Koopman was able to connect directly to the remote host computer located at IP Address 174.51.59.13 and was placed in queue to receive the file. The suspected child pornography file that Detective Koopman placed into queue to download was called “- (SDPA) nena 5Yo (4).avi”.
 - C. During Detective Koopman’s connection to the user client at IP Address 174.51.59.13, it was logged that the user client had the complete file available for download and that the file size was 328015872 bytes. The user client identified the file with an eD2k MD4 hash value of 99E58B5D2C716FF33552890461D2A024.
 - D. Detective Koopman’s client program remained in queue to receive the aforementioned file until May 6, 2012 at 09:56:00 when the connection was terminated by the user client at IP Address 174.51.59.13. Your Affiant was unable to complete this download and did not receive enough of the file for it to be played or viewed.
 - E. On July 13, 2012, Detective Koopman located the same file identified as “- (SDPA) nena 5Yo (4).avi” through the eD2k Network and downloaded it from another source. Detective Koopman downloaded the complete file and noted that it had the same name, was the same size, and also has the exact same eD2k MD4 hash value of 99E58B5D2C716FF33552890461D2A024. The fact that the eD2k MD4 hash values match exactly means that there is only approximately 1 in 9.2 quintillion chance that the file is anything different than the file downloaded from IP Address 174.51.59.13. In other words, this method of comparison is 9 times more accurate than matching DNA profiles in human beings.
 - F. On July 18, 2012, your Affiant viewed portions of the movie file “- (SDPA) nena 5Yo (4).avi” with the MD4 hash value of 99E58B5D2C716FF33552890461D2A024, which is approximately 33:46 minutes in length. The movie depicts multiple nude minor females on or near a bed masturbating with their fingers and inserting various dildos, sex toys and other objects, such as a wine bottle-like object, into their vaginas. The video concludes with a minor female performing oral sex on a nude minor female lying on a bed.
25. A federal search warrant was obtained for the residence at 8034 East Fairmount Drive, Denver, Colorado 80230 and was executed on July 24, 2012. Upon entry, Mr. Moe was found alone in the home.
 26. Mr. Moe was advised of and waived his *Miranda* rights. He stated that he is the sole resident of the home. He admitted that he used the peer to peer program and the Internet to make available, trade, and collect images of child pornography. He stated he was running two peer to peer programs: eDonkey and WinMX. He also admitted to possessing child pornography on his computer.
 27. With regard to his employment at Paddington Station, Mr. Moe stated that he has been a teacher at Paddington Station for the last 18 years. Mr. Moe stated that during the course of his career, he has seen children in his care nude, either changing into their swimsuits or when he has assisted them with going to the bathroom. He stated that policies at the school have changed over the course of the last eighteen years

and he also stated that under current policies at Paddington Station, only females are allowed to change diapers and two adults must escort children to the bathroom.

28. Mr. Moe also stated that he first started working with children in 1990 at Racketworld in Denver, Colorado and as a lifeguard at the Jewish Community Center in Denver, Colorado.
29. Mr. Moe was shown portions of the movie file “- (SDPA) nena 5Yo (4).avi” with the MD4 hash value of 99E58B5D2C716FF33552890461D2A024. Mr. Moe recognized the movie file as one he possessed, but did not remember where it was on his computer or where he got it, though stated it was through a “video sharing site.” Mr. Moe stated that he has lots of sexually explicit images, approximately 10,000, and estimates that 2% depict children under the age of 18. Mr. Moe’s preference is to look at sexually explicit images depicting females ages four and older.
30. Two computers were located at the address. Mr. Moe stated that both computers belonged to him. A preview has been conducted on one of the two computers, namely a desktop computer located on a desk in the second floor loft area. The desktop computer was powered off at the time of the search warrant execution and was connected to the Internet through a wired connection. Based on the preliminary preview, numerous folders containing child pornography were present on the desktop of Mr. Moe’s desktop computer. Child pornography file names included, for example, the term “PTHC,” which is a term associated with the collection of child pornography. Based on my training and experience, “PT” refers to “pre-teen” and “HC” refers to “hard core,” which refers to images depicting sexual acts. At least 12 videos located on the desktop computer match an ICE database of known or suspected child pornography previously encountered by law enforcement. The hard drive from the desktop computer that was previewed bears the inscription “Product of China.”
31. During the execution of the search warrant, a box containing at least 500 DVDs and/or CDs was located. At this point in time, approximately 15 of the DVDs/CDs have been reviewed and contain files depicting a mixture of child pornography and adult pornography.
32. During the execution of the search warrant, handwritten notes were found. Mr. Moe stated that the notes involved an incident regarding a three (3) year old female minor and that the incident had occurred approximately ten (10) years ago. Mr. Moe further stated that a child in his care at Paddington Station said that he had taken her to the bathroom and touched her inappropriately. Mr. Moe further stated that nothing was proven and that the notes were taken during the meeting with the child’s parents.
33. During the execution of the search warrant, the guest room closet was found to contain sheets fitted for a toddler bed or crib, though Mr. Moe does not have children nor was a toddler bed present at Mr. Moe’s home. Some of the sheets appeared rumpled and/or stained. Mr. Moe explained that he keeps the sheets on hand in the event children at the school need sheets.

CONCLUSION

34. Based on the investigation described above, I believe that there is probable cause to believe that the defendant has committed violations of Title 18, United States Code, Sections 2252A(a)(2), distribution and attempted distribution of child pornography, and 2252A(a)(5)(b), possession of child pornography .

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.

s/Melissa Coffey

Melissa Coffey, Special Agent
Immigration and Customs Enforcement
Homeland Security Investigations

Jul 24, 2012 6:34 pm

SUBSCRIBED and SWORN before me this _____ day of _____ 2012



UNITED STATES MAGISTRATE JUDGE

Kathleen M. Tafoya
United States Magistrate Judge

DEFENDANT: DAVID PAUL MOE

YOB: 1966

ADDRESS Denver, Colorado

OFFENSE(S): **Count 1:** Distribution and Attempted Distribution of Child Pornography, Title 18, United States Code, Section 2252A(a)(2) and (b)(1).
Count 2: Possession of Child Pornography, Title 18, United States Code, Section 2252A(a)(5)(B) and (b)(2).

LOCATION OF OFFENSE: Denver County, Colorado

PENALTY: **Count 1:** For first offense, NLT 5 years and NMT 20 years imprisonment, NMT \$250,000 fine, or both; supervised release of NLT 5 years and NMT life; \$100 Special Assessment. If defendant has a prior conviction under Title 18 Chapters 110, 71, 109A, or 117; Title 18 section 1591; or under Section 920 of Title 10 of the United States Code (Article 120 of the Uniform Code of Military Justice); or under the law of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment or transportation of child pornography, or sex trafficking of children, NLT 15 years and NMT 40 years imprisonment, NMT \$250,000 fine, or both; supervised release of NLT 5 years and NMT life; \$100 Special Assessment.
Count 2: For first offense, NMT 10 years imprisonment, NMT \$250,000 fine, or both; supervised release of NLT 5 years and NMT life; \$100 Special Assessment. If defendant has a prior conviction under Title 18 Chapters 110, 71, 109A, or 117; or under Section 920 of Title 10 (Article 120 of the Uniform Code of Military Justice); or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment or transportation of child pornography, NLT 10 years and NMT 20 years imprisonment, NMT \$250,000 fine, or both; supervised release of NLT 5 years and NMT life; \$100 Special Assessment.

AGENT: Special Agent Melissa Coffey
ICE HSI

AUTHORIZED BY: Alecia Riewerts Wolak
Assistant U.S. Attorney

ESTIMATED TIME OF TRIAL:

X five days or less

THE GOVERNMENT

X will seek detention in this case

The statutory presumption of detention is applicable to this defendant.

OCDETF CASE: ___ Yes X No